第4章

システムLSI設計における DPA対策の指針と AES暗号の対策例

―― 対策の有効性と回路コストのバランスをじょうずにとる

森岡澄夫

暗号処理回路は，それ単体で1チップ化されることは少なくなり，今日ではシステムLSIに組み込まれて使われる場合が大半です．システムLSIの実装には，FPGAを使うケースもありますが，通常はスタンダード・セル（セル・ベースIC）を使います．また，暗号の種類について，電力解析の学術論文では旧来のDES（Data Encryption Standard）がよく使われていますが，実務ではAES（Advanced Encryption Standard）などへ移行しています．本稿では，こうした動向を受け，一般のシステムLSI設計における電力解析攻撃への対策方針と，システムLSI上のAES暗号回路の攻撃対策法を紹介します．（著者）

電力解析攻撃[注1]は，暗号回路実装の研究において，ここ数年ホットな話題です．暗号数理の高度な知識や高価な機器を用いなくても攻撃可能という点で驚くべきテーマであり，暗号研究者以外の人にも比較的知られるようになってきました．

1 実設計時の電力解析攻撃と対策

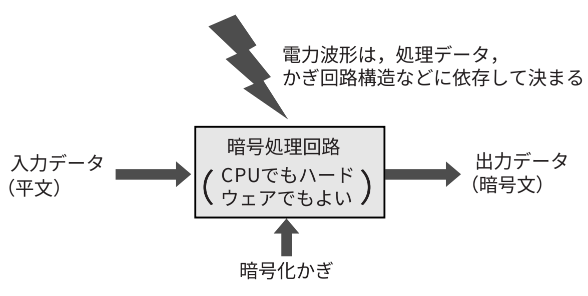
ここで，電力解析攻撃について簡単におさらいします（**図1**）．おおかたの回路では，その動作中の電力波形は，処理するデータの値や回路構造に依存して決まります．この性質を利用し，電力波形の測定結果から，暗号回路にセットされているかぎ（これもデータの一種）を推定するのが，電力解析攻撃です．

注1：本稿では，SPA（simple power analysis），DPA（differential power analysis），EMA（electromagnetic analysis），DEMA（differential electromagnetic analysis）などを総称して「電力解析攻撃」と呼ぶことにする．

● 学術論文と通常のLSIには多くのギャップがある

言うまでもなく，学術論文と通常のシステムLSIの間には，設計条件などにかなりのギャップがあります（**表1**）．学会で発表される攻撃対策法（以下，単に対策法）には，コストがかかり過ぎたり，あるいはシステムLSI設計の観点からは非現実的であったりする場合があります．攻撃に過度におびえて回路コストを不必要に跳ね上げる対策法を使うのも，逆に，すっかり無関心になって何も対策しないのも，どちらも好ましくありません．

通常のシステムLSI設計でどう対策に取り組むべきか，確立された方法論はまだありません．本稿では，筆者の私見を記します．あくまで，個人的な見解ですので，みなさんが自分の設計に適用するときは，よく吟味し直してください．



- データ値と電力波形から，かぎを推定
- 波形は電流計で直接測ってもよいし（SPA，DPA），電磁波で間接的に測ることも可能（EMA，DEMA）
- 処理時間の変化から，かぎがわかる場合がある（タイミング・アタック）
- 1回の演算処理波形から，かぎがわかる場合がある（SPA，EMA）
- 多数回の演算処理の平均波形から，かぎがわかる場合がある（DPA，DEMA）

図1　電力解析攻撃の概要

暗号処理回路（CPUでも専用回路でもよい）の電力波形が，入力データやかぎ，回路構造などに依存することを利用して，電力波形からかぎの値を推定する．どのような方法で推定するかは，いろいろバリエーションがある．

4

表1　研究レベルと通常のシステムLSI設計のギャップ

電力解析攻撃と対策の研究が盛んだが，学術研究は自由な仮定のもと，さまざまな手法を探るものなので，通常のシステムLSI設計の条件とはギャップがある．一般的なシステムLSIにはとても使えない手法の提案も多いが，LSIの設計ルールも攻撃手法も時代とともに変化するので，「研究は役に立たない」と全部無視してしまうのは危険．なお，現時点において，90nmなどの微細プロセスで製造したシステムLSIを，実際に電力解析攻撃できたという報告は，筆者は聞いたことがない．防御法についても，当然ながら完ぺきなものは存在しない．

	研究レベルの話	通常のシステムLSI	備　考
暗号回路のサイズ	チップ全体または大半	ごく一部	システムLSIでは，暗号回路の消費電力は，ほかの回路のそれに隠されてしまいがち
デバイス	FPGAもしくは旧プロセスで評価（0.5 μm～0.25 μmなど）	最新のものは90nm～65nmの設計ルールで製造	微細化すると，消費電力もチップ上の面積も小さくなるので，攻撃は難しくなる
テクノロジ・ライブラリ	暗号部には専用のセル・ライブラリが使える	暗号部だけ別ライブラリで設計することは，まず不可	—
回路の設計抽象度	どれだけ下位でも可（トランジスタ・レベルなども可）	通常はRTLが最下位．今後は，ビヘイビア合成の利用も考えられる	—
非同期論理回路	使用可能（dual rail方式など）	原則，使用不可	—
回路の処理クロック数	動的にランダムに変えてよい	原則，固定したい	システム処理性能が予測不能では困る
データ（平文，暗号文）の観測	暗号IPの入出力データ値を，外部で観測できる．または外部から制御できる	暗号IPの入出力は，外部から観測も操作もできない場合が多い	データ値が不明でも攻撃可能な場合がある，との報告が最近あった
暗号のかぎ設定	一度セットしたら，ずっと同じ値のままと仮定する	システムによっては，どんどんかぎを切り変えてもよい場合がある	DPA，DEMAにおけるかぎ導出には，同一かぎで，数百回以上の暗号処理が必要
電力の測定精度	どのような微小電力，高速変化でも測定可と仮定する	微小，または高速な変化は，安価な装置では測定不能	—

● **電力解析攻撃はシステムLSIにとって脅威なのか？**

システムLSIといっても多種多様であり，電力解析攻撃が脅威なのかどうか，断定的に“Yes”，“No”を言うことはできません．しかし，少々粗い議論ですが，以下の条件をいくつか満たすならば，今すぐの脅威とはならないでしょう．

- **90nmや65nmといった最近の微細プロセスのスタンダード・セルを使っている**—— 微細プロセスでは，暗号回路の平均消費電力は数百μW～十数mWのオーダになり，しかもリーク電流などの割合が高い．電力解析攻撃に使えるのはゲートのスイッチング動作による消費電力のうち，データ値に依存して変わる電力差であるが，それは数μW～数百μWといった微小なものになる注2．
- **暗号処理部が回路全体のごく一部である（図2）**—— 全体の消費電力から暗号処理の分を抽出するためには，多量のデータ・サンプリングが必要になる．
- **暗号演算を専用回路で行っている**—— CPUで行っているならば攻撃されやすいかもしれない．一般に，プロセッサ処理は電力解析攻撃に弱いという傾向がある．
- **かぎを頻繁に変更している**—— DPAやDEMAでは，同じかぎのままで，暗号演算を最低数百回はサンプリングする必要がある．
- **暗号処理がいつ行われているかを正確に（クロック精度で）とらえることが難しい**—— これがわからないと，どの時点の電力波形をサンプルしてよいかわからず，攻撃できない．ただし，暗号処理実行のタイミングを割り出すような方法の研究も行われている．
- **暗号処理の入出力データ値（平文や暗号文）をチップ外部から直接観測できない，もしくは外部から制御できない**——ただし，それでも適用できる攻撃法の研究もある．

以上の条件から大きく外れる場合，電力解析攻撃は脅威となりえます．もちろん，ある製品に搭載したシステムLSI

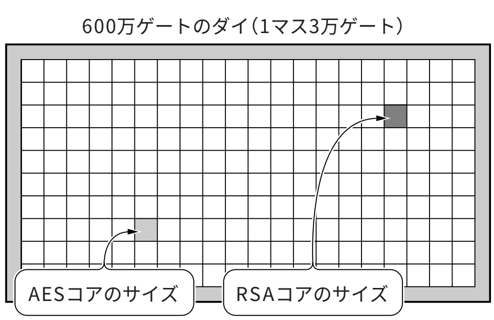


図2　一般的なシステムLSIでは，攻撃の対象となる暗号IPは全体のごく一部でしかない

電力解析攻撃のターゲットは，AESやRSAといった暗号処理部である．CPUでなく専用回路で暗号演算を行う場合，どのような暗号でも2万～4万ゲート程度の回路規模なので，システムLSI全体のうち，図に示す程度の割合しかない．また，65nmや90nmといった微細なプロセスでは，暗号回路の平均消費電力は数百μW～十数mWしかない．したがって，暗号処理を専用回路で実行しているかぎり，電力解析攻撃は現状では相当難しく，今後はさらに難易度が上がる傾向にある．ただし，CPUで暗号演算を行ったり，FPGAを使ったり，あるいは古いプロセスを使うならば話は別である．

注2：しばしば誤解されるが，「微小電力だから攻撃できない」ということではない．十分に精密な電力測定環境を用意し，十分に多量のデータ・サンプリングを行えるならば，攻撃そのものは可能である．そのためにかかるコストが現実的なものかどうかが，脅威か否かの判定基準である．

が現時点で攻撃できなくても，5年後や10年後になって攻撃されて問題となるリスクはあります．これについては正確に予測できません．

● 対策法にはシステムLSI設計と相いれないものも多い

電力解析攻撃に対する対策法には，大きく分けて次の三つのアプローチがあります．

- **暗号回路の消費電力がデータ値によらず一定になるようにする**——暗号専用のセル・ライブラリの利用や，非同期回路（dual rail方式）の利用，レイアウトのくふうなど
- **電力波形とデータ値の相関関係をかく乱する**——ランダム・マスク手法（詳細は第2章，Appendixを参照）など
- **電力波形を時間軸上で変形させる**——演算処理時間をランダムに変える，非同期回路の利用など

より正確な分類や各対策法の詳細については，参考文献(1)，(2)などを見てください．ほとんどの対策法は，回路規模が数倍になる，クリティカル・パス遅延が数倍に増える，消費電力が数倍になる，回路設計作業が著しく難しくなる，といった何かしらの悪影響を及ぼします．

回路規模や速度といった量的な影響だけならば，まだマシなほうだと言えます．研究レベルの対策法の中には，現在のシステムLSI設計手法と相いれないものもあります（**表1**）．例えば，非同期回路や暗号専用カスタム・セル，あるいは特殊なレイアウト手法を用いたりする対策法は，通常のシステムLSI設計においては設計技術と開発体制の両面から容認しがたいものでしょう．これらの方法をチップ全体でなく暗号回路部だけに用いることも，「回路開発上のリスク≪セキュリティ上のリスク」であるとうまく説明できないかぎりは，認められないケースが多いのではないかと思います．

● 時代逆行（？）はしかたのない面もある

対策法にシステムLSIの動向と相いれにくい一面があることは，ある程度はやむをえません．攻撃を防ぐためには電力波形を適切に制御する必要がありますが，そうしようとすれば，回路の動作タイミングや論理構成に細心の注意を払わざるをえなくなるからです．

システムLSI設計技術は，ビヘイビア合成や論理合成などによって，動作タイミングや回路構成を隠ぺいしていく方向で進んでいます．しかし，これらがまさに電力解析攻撃でねらわれる部分なのです．高位設計ツール任せで回路を設計すると，攻撃が容易になる可能性があることを知っておいて損はないでしょう．この点については，後で例を示して説明します．

● 実設計時における六つの対策指針

ではここで，システムLSI設計において電力解析攻撃にどのように対応するか，筆者の私見を整理します．

1) 対策はいわゆる「保険」と同じように考える．扱う情報にどれだけの価値があり，何年後まで守るべき情報で，攻撃してくるのがだれで，セキュリティが破れた場合の被害は何か，といった点から対策に払うコストを決める．
2) 今のところ，電力解析攻撃などよりも，システムLSIのアーキテクチャ設計やソフトウェア実装に由来する脆弱性（バッファ・オーバフローなど）のほうが緊急の脅威である．
3) 理論的に100％完全な対策法は知られていない．しかし，「完ぺきでない対策はむだ」と"all or nothing"で考えるのはよくない．対策によって攻撃の難易度を引き上げることに大きな意味がある[注3]．
4) 対策としてもっとも有効なのは，プロセス微細化と専用回路化である．システムLSIで行うセキュリティ関連処理のうち，最低でも暗号演算だけはCPUで

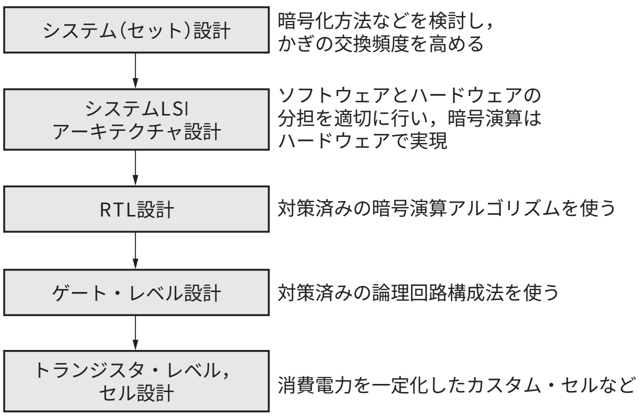


図3　電力解析攻撃の防御のための各設計レベルにおける検討事項

上位設計レベルほど，個々のシステムに固有な対策となる．下位レベルの対策法は一般的なシステムLSIの設計ではあまり使えず，RTLかゲート・レベルまでが実質的な下限である．どこか一つのレベルで完ぺきな対策を打とうとするのではなく，複数のレベルで複合的に対策するほうがよい．

注3：電力解析攻撃が注目されるのは，オシロスコープと簡単なプログラムを用意するだけで多数の人が攻撃に参加しうるからである．実際のシステム設計では，セキュリティの専門家でない人が今後5～10年ほど攻撃できないレベルまで対策すれば十分，という場合が多い．

4

なく専用回路で行う（それだけで攻撃は数段難しくなる）．そのうえで，発表されている対策法をコストに見合う範囲で施しておく．

5）一つの対策に頼り切らず，複数の対策を併用する（**図3**）．ガードを増やす意味合いがある．また，ある設計レベルだけで対策しようとするとコストがかかるが，別のレベルで対策すれば簡単に済む，ということもよくある注4．

6）システムLSIの標準設計フローから大きく外れる対策法は，できるだけ避ける．上流設計レベルの対策をメインとし（詳細は後述），バックエンドでの対策法は避けるほうがよい．

2 シミュレーションによる電力解析

次に，システムLSI用暗号回路の具体的な電力解析攻撃対策について説明します．

● 設計の上流工程で電力波形を予測したい

システムLSIに暗号処理回路を搭載する場合，施した攻撃対策の有効性を，設計の上流工程である程度確認する必要があります．回路の速度や規模などと同じことですが，実チップになるまでまったく評価できないというのでは，非常に困ってしまいます．

評価のためには，回路の電力波形をなんらかの方法で予測する必要があります．ところが，回路の速度や規模などと異なり，電力波形を予測するようなEDAツールはあまりありません（平均スイッチング確率を与えて平均消費電力を見積もるツールはよくあるが，攻撃対策の評価には使えない）．

なお，FPGAによるプロトタイピングは電力解析攻撃の評価に適しているとは言い難いものです．こと暗号回路の消費電力については，FPGAとスタンダード・セルでは挙動が大きく異なるためです注5．

● シミュレーションを使った電力波形予測

図4に，広く普及しているEDAツールを使って予測波形を作る方法を紹介します．ここで行おうとしていることは，「論理ゲートのスイッチング回数の変化を電力波形とみなす」というもので，それ自体は別に目新しくありません．

具体的な手順としては，まず暗号回路を論理合成してネットリストとSDF（回路遅延情報）を作成し，遅延シミュレーションを行います．これにより，ゲートのスイッチング・ログが得られるので，一定時間間隔（値は任意）で累算したスイッチング回数のグラフを作ると，それが予測電力波形となります．スイッチング・ログは，VCD（value change dump）と呼ばれるシミュレータ非依存の統一フォーマットで生成すると扱いやすいでしょう（**図5**）．なお，

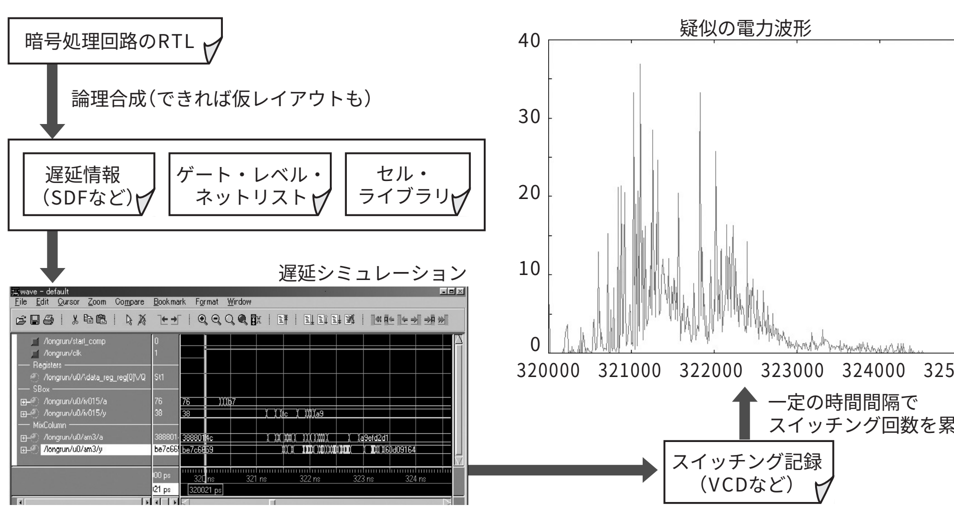


図4
システムLSI用暗号回路の電力波形の疑似測定環境
システムLSIに搭載する暗号回路については，電力解析攻撃対策が有効かどうかを，チップ作成前に評価したい．とくに暗号回路では，FPGAプロトタイピングによる評価より，回路シミュレーションによる評価のほうがずっと正確と思われる．もちろん，シミュレーション上で攻撃できなかったからといって，安全が保証されるわけではない．シミュレーションはあくまで，防御法の有効性確認の補強材料である．

注4：例えば，1回暗号処理するたびにかぎを変更できるようなシステムだったとして（それだけでDPA攻撃やDEMA攻撃はほぼ無理になる），これを知らない回路設計者が多大な労力を払ってカスタム・セル設計などで対策しても，コストとリスクが増えるだけである．
注5：XOR演算が多用される暗号回路は，FPGAの基本プリミティブであるLUT（look-up table）と相性が悪い．そのため，同じRTLでも，マッピング後の回路構造がスタンダード・セルの場合と著しく異なったものになる．

仮配線を施してから遅延情報のバック・アノテーションやSPICEシミュレーションなどを行えば，より実際に近い波形になります．

もちろん，得られた電力波形は，実回路における波形とは異なります（**図6**）．「シミュレーション波形で攻撃できなければ，実チップでも攻撃できない」ということではありません．したがって，きちんとした理論的裏づけのある対策を行い，その有効性を確認する手段としてシミュレーションを用いるべきです．

● AES暗号回路に対するDPA攻撃のシミュレーション

AES暗号回路の予測電力波形を実際に作成してみた例を，**図7**に示します．得られた波形（**図7**の下段）に対して，電力解析攻撃を行うことができます．

今回は攻撃の種類の一つ，DPA（differential Power analysis）を行ってみました．DPAについての簡単な説明は次のとおりです（詳細は，本特集第2章，第3章，および参考文献(2)，(3)を参照のこと）．

- 組み合わせ回路の消費電力は，通常，その入力値によっ

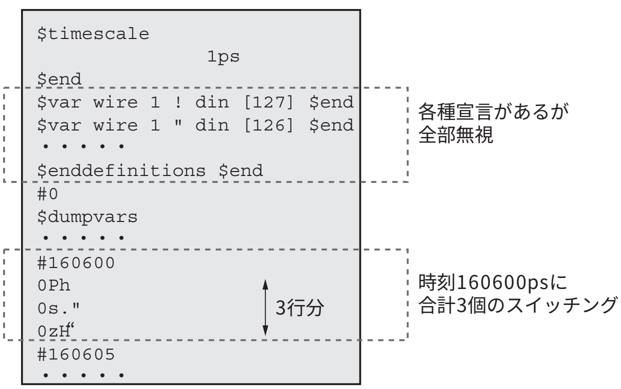


図5　VCDファイルからスイッチング回数を読み取る

VCDファイルには，どの時刻にどの信号線の値が変化したかが記録されている．スイッチング回数を調べるには，簡単な行数カウント・プログラムを作れば十分．

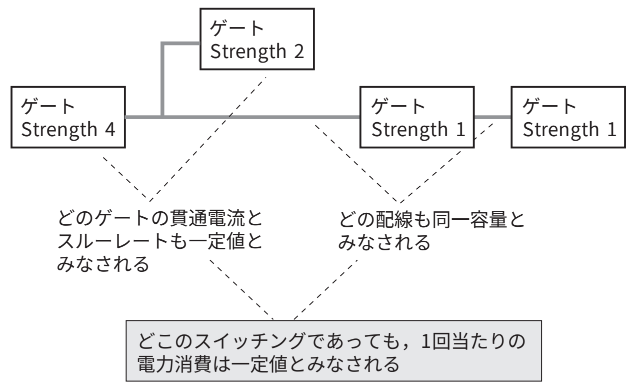


図6　スイッチング回数から電力波形を予測する場合の誤差

スイッチング回数のみから電力波形を予測する場合，どのゲートでも1回のスイッチングで消費される電力が一定，という仮定があることに注意．実際には，配線容量やそのほかの違いがあるので一定ではない．

4

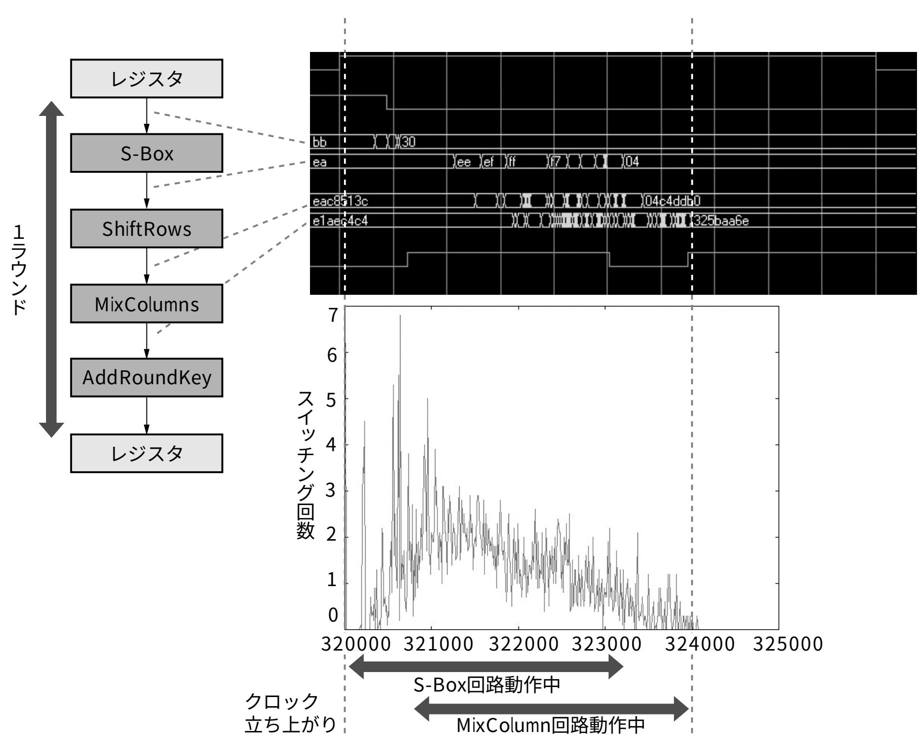


図7
AES暗号回路における1ラウンド分の電力波形の例

典型的なAES回路では，「ラウンド」と呼ばれる演算処理を1クロックに1回行う．1ラウンド分の演算が組み合わせ回路になるが，回路内部の信号伝播時間差からダイナミック・ハザードがたくさん発生し（図の上段のシミュレーション波形），クロックが立ち上がった後のスイッチング回数変化は図下段のように時間幅を持つ．

て異なる．回路内部におけるゲートのスイッチング確率や信号変化の伝播経路が，入力値に依存するからである

- 入力値による消費電力の違いが非常に大きいなら，1回の暗号演算の電力波形からそのまま暗号化のかぎを読み取れることがある（これがSPAやEMA）
- 違いが微小であっても，多量の演算を行って平均の電力波形をとると，入力値による差分が現れるのでかぎを推定できる（これがDPAやDEMA．**図8**）

図9に，シミュレーションでAES暗号回路の予測電力波形を作り，DPA攻撃に成功した例を示します．図において，実線のグラフは推定が正しい場合の差分を表しています．一方，「＋」で示されているグラフは誤って推定した場合の差分です．なお，この実験には約1GHz動作のパソコンで数十分の時間，および数十Gバイトのハード・ディスク容量が必要でした（遅延シミュレーションにいちばんコストがかかる）．実用的なコストで評価できると言えます．

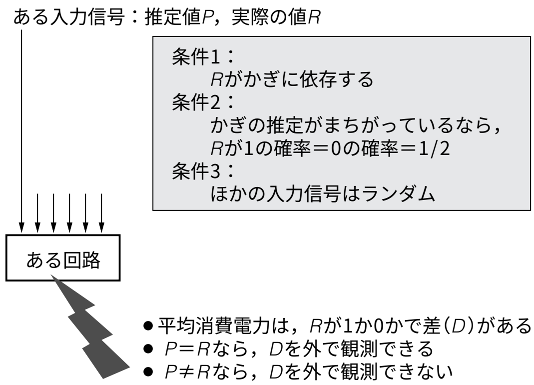


図8　DPA攻撃の原理

組み合わせ回路のある入力ビットAについて，ほかの入力ビットをランダムとみなせる状況下で多量のデータを流し，平均消費電力を測定すると，普通，A＝1のときとA＝0のときで消費電力が異なる．これを応用してかぎに依存する信号の値を推定し，電力差を検出できるか否かで推定の正誤を判定する．

● 論理回路の構造と電力解析攻撃のやりやすさ

AES暗号回路の場合，その電力の大半はS-Boxと呼ばれる組み合わせ回路で消費されています．したがって，S-Boxの回路構成によって電力波形が大きく変わり，攻撃の難しさも変わります．

図10にその例を示します．S-Boxは8ビット入出力の組み合わせ回路ですが（一般的なAES回路では16個使われる），これを積和形の回路で作った場合，1,000回程度の暗号化処理の平均電力波形でDPA攻撃できます．これに対し，BDD（binary decision diagram；二分決定グラフ）をもとにセレクタ・ベースで作った場合は，10,000回でもまだ攻撃できません（もっと多量の演算が必要）．このような結果になるおもな理由は，セレクタのスイッチング確率にセレクト信号値による偏りがなく，S-Box全体でも入力値による消費電力差が小さくなるためだと推定できます．

さて，組み合わせ回路を作るとき，テーブル（真理値表）

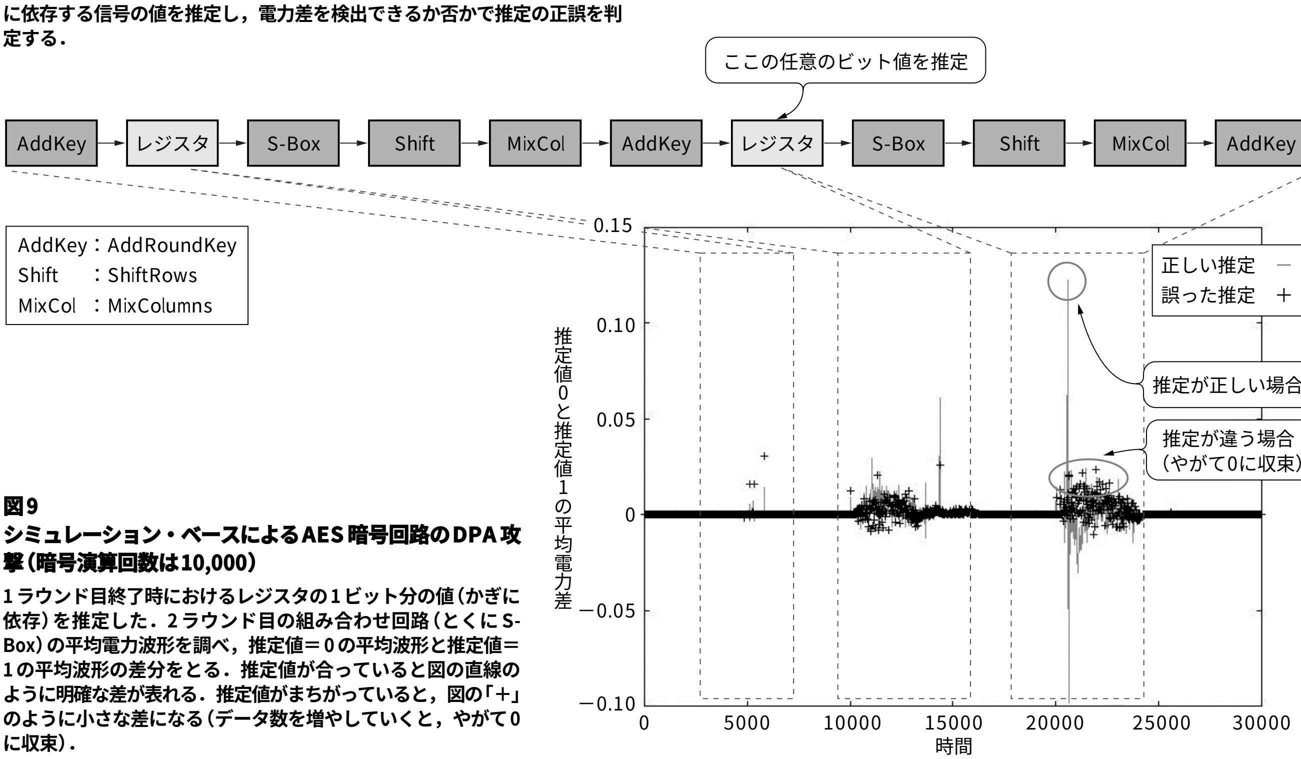


図9
シミュレーション・ベースによるAES暗号回路のDPA攻撃（暗号演算回数は10,000）

1ラウンド目終了時におけるレジスタの1ビット分の値（かぎに依存）を推定した．2ラウンド目の組み合わせ回路（とくにS-Box）の平均電力波形を調べ，推定値＝0の平均波形と推定値＝1の平均波形の差分をとる．推定値が合っていると図の直線のように明確な差が表れる．推定値がまちがっていると，図の「＋」のように小さな差になる（データ数を増やしていくと，やがて0に収束）．

から自動論理合成してしまうことがよくあります．回路設計者は，合成ツールがどのような回路を生成するかなど気にとめないでしょう．しかし，**図10**のような大きな違いが出てきかねないので，電力解析攻撃のターゲットになりそうな回路の作成は，ツールに完全に任せ切らないほうがよいでしょう．

4 AES暗号のRTL対策法

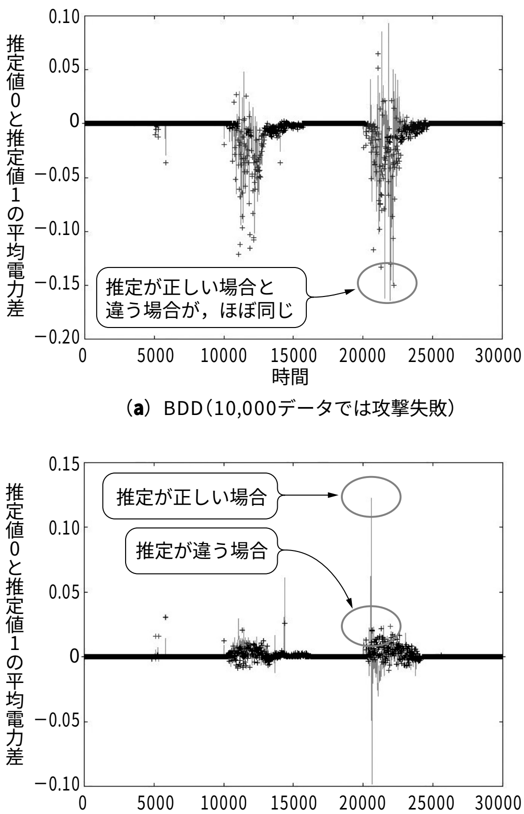
AES暗号回路について，大半のシステムLSIで問題なく使えると考えられる攻撃対策法を紹介します．パテント・フリーであるうえ，RTLで対策でき，コストもそれほどかからずに済みます．

● ランダム・マスク法の基本的なアイデア

ここでは，いくつかある対策法のうち，「ランダム・マスク法」と呼ばれるものを使います（**図11**）．そのアイデアは，**図11（b）**のように回路内のワイヤ値を「本来の値＋乱数X」とすることです（なお，ここではガロア体の演算を行っているので，＋は整数加算ではなくXORを意味する．以下同じ）．電力波形が乱数Xによってかく乱されるので，攻撃が難しくなります．なお，乱数Xは外部で生成し（できれば疑似乱数でなく，物理乱数がよい），AES暗号処理を1回行うごとに切り替えます．

もちろん，普通のAES暗号回路に対して「平文＋X」を入力してしまっては，出力から暗号文を抽出できません．このため「暗号文＋X」が出力されるように内部演算を数学的に改造するのですが，これがいちばん難しいところです[注6]．AESでは以下に紹介する方法でうまく改造できているのですが，DESなどでは数学的改造が難しく，回路をプログラマブル化するという代替法があります（**図12**）．こ

注6：$D+X$から$f(D)+X$を数学的に求めることができるかどうかが問題である．ここで，「$D+X$とXから元のDを求め，$f(D)$を計算し，Xを足して$f(D)+X$に戻す」などとしては，$f(D)$計算の消費電力が乱数でかく乱されず，何の意味もなくなってしまう．それゆえに難しい．

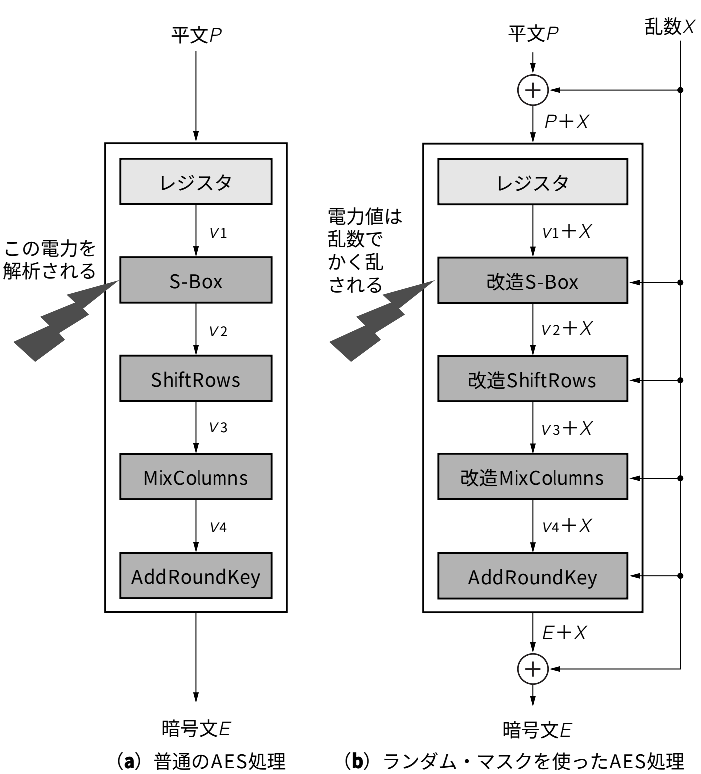


（**a**）BDD（10,000データでは攻撃失敗）

（**b**）積和形（10,000データでも攻撃成功）

図10 AESのS-Boxの論理回路構成による攻撃難易度の変化

同じ演算を行う回路でも，その論理回路構成方法はいくつもある．入力値が違っても消費電力があまり変わらないような回路構成にすると，電力解析攻撃は行いにくくなる．

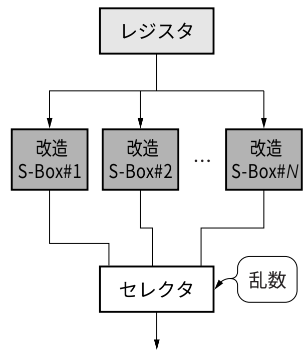


（**a**）普通のAES処理　（**b**）ランダム・マスクを使ったAES処理

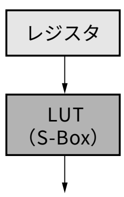
図11 電力解析攻撃に対する現実的防御法「ランダム・マスク」

電力解析攻撃に対する対策法のうち，通常のシステムLSIにもっとも適していると思われるのがランダム・マスク法である．これは，暗号演算の中間値に乱数をXORした状態にするものである．乱数は1回の暗号処理ごとに切り替える．電力波形が乱数でかく乱されるので，攻撃がとても難しくなる．正しい演算結果が得られるように，内部演算回路の改造が必要．

4



（a）複数のS-Boxを乱数で切り替える



（b）S-BoxをLUTにして，随時書き換え

図12　ランダム・マスク法の一種のアレンジ（AESでは使わない）

乱数を加えたデータに対して正しく演算できる回路を，つねに組めるとは限らない．その場合，（a）のようにXORする乱数値を限定してすべてを回路化する，または（b）のように回路をプログラマブル化してしまう，という代替法がある．いずれも回路規模が増大する．

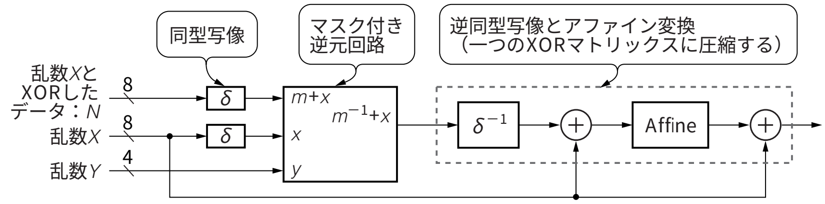


図13　ランダム・マスク用AES S-Box回路

入力データをD，乱数をXとしたとき，$D+X$を入力として，S-Box（D）＋Xを出力する回路である．ガロア体の同型性を使い，合成体と呼ばれる体の上で演算する．

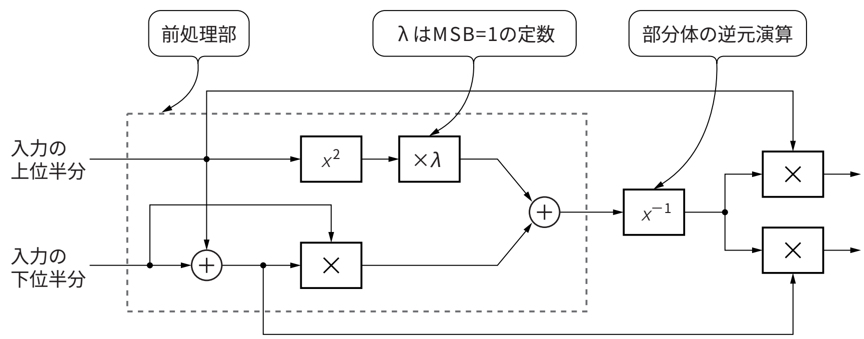


図14　合成体$GF(((2^2)^2)^2)$上の逆元演算回路（マスクのない通常AES用）

部分体$GF(((2^2)^2)^2)$の演算回路の組み合わせである．図中の$GF(((2^2)^2)^2)$の逆元演算は，その部分体$GF(2^2)$の演算回路を用い，この図とまったく同じ構成で作る．

の場合，コスト的に大きな負担がかかります．

● 現在知られている手法の限界

実は，ランダム・マスク法に完全なものはまだ存在しません．「理論的に攻撃不能となるわけではないが，攻撃難易度は大幅に向上する」という理解のもとで使ってください．専門的になりますが，これから紹介する方法も次の点で完全ではありません（現時点で学会において議論されつつあるところ．参考文献(5)なども参照）．

- 高階差分攻撃（HO-DPA）と呼ばれるものには対策できていない
- 回路の形式モデリングに実際と異なる面がある．「ゲート遅延＝0，スイッチング確率のランダム性＝ワイヤ値のランダム性」という仮定がなされている

ただし，後述しますが，不完全だから無意味だというわけではなく，実際にはかなりの効果があります．

● AES回路のランダム・マスク化

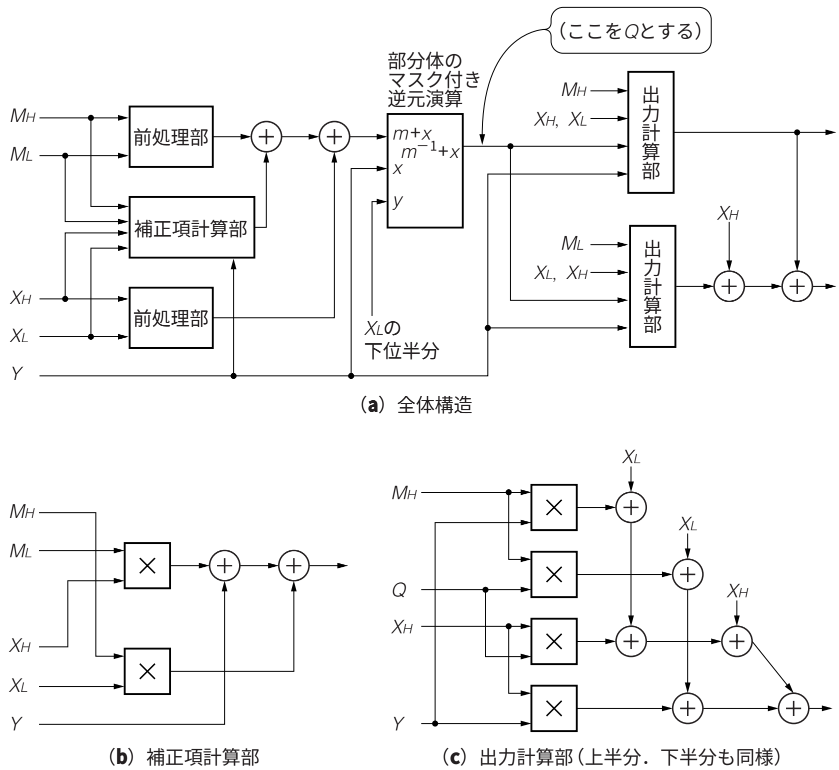
それでは，ランダム・マスク手法を導入したAES暗号回路について説明します．

全体構成は**図11**のとおりですが，外から与える乱数として，128ビットのXだけでなく，64ビットのYも追加します．平文にXORするのはXで，YはAES内部で使います．

かなめとなるのは，S-Box（正確にはSubBytes）の構成法ですが，それは後述することとし，ほかの基本演算の構成について先に説明します．まず，AddRoundKeyについては，単なるXORなので改造の必要はありません．MixColumnsについては，「MixColumns（入力＋X）＋X」という回路をまず構成します．これはXORマトリックスになるので，XORをとる順番を入れ替え，乱数XのXORを最終段で行う形にします．ShiftRowsもMixColumnsと同じように改造します．

● 合成体を使ったランダム・マスク用S-Box

図13に，ランダム・マスク用のS-Boxの回路構造を示します．この回路は，8ビットのデータD，8ビットの乱数X（回路に与えられた128ビットのXの一部のこと），4ビットの乱数Y（これも与えられたYの一部）に対し，｛$D+X$，X，



◀図15 合成体 $GF(((2^2)^2)^2)$ 上の逆元演算回路(ランダム・マスク用)

マスクのない場合と同じで，部分体の演算回路を使って再帰的な構成で作ることができる．演算の接続順序は，この図のとおりにすること．

表2 ランダム・マスク用AES S-Boxの回路性能の例

回路の遅延はやや大きめになるが，問題ない範囲である．ランダム・マスク法を採用したにもかかわらず，マスクなしの場合と比べても大差ない規模のAES回路を作ることが可能．

	回路遅延(ns)	回路サイズ(2入力NAND換算)
合成体(マスクなし)	2.2	354
BDD(マスクなし)	0.7	1,399
積和形(マスクなし)	0.7	1,650
合成体(マスクあり)	4.5	1,300

Y}の三つを入力としてS-Box(D)＋Xの値を出力します．

S-Boxの内部演算には，ガロア体の一種である合成体というものを使います．S-Boxはガロア体の逆元演算に補助演算を追加したものですが，合成体を使うと際立って小規模な回路になるという特徴があります(詳細は参考文献(6)～(9)を参照)．

普通のAES用の逆元回路を**図14**に，ランダム・マスク版AES用の逆元回路を**図15(a)**に示します．**図15(a)**の回路では，**図14**の前処理部を二つ使います．その内部回路は**図14**と同じです．また，補正項計算部(**図15(b)**)というブロックを追加します．**図14**における部分体の逆元演算は，部分体のマスク版逆元演算に置き換わります．つまり，マスクなしの場合と同じく，再帰的な回路構造をとります．**図14**の終段の乗算器は，出力計算部(**図15(c)**)というブロックに置き換わります．

以上の回路がどのような考えかたで設計されているのかについては，参考文献(4)を参照してください．

● マスクありでも規模，遅延ともに問題なし

S-Box単体の回路性能を**表2**に示します．回路規模は，普通のAESで使われる自動合成S-Boxと比べて大差ありません．遅延はやや増えますが，大きな問題になるほどではありません．AES回路全体では，攻撃対策を施していないAES回路に劣らない回路性能を達成できています．合成体を使わなければ，**図12**に示した方法をとらざるをえなくなるのでこうはいきません．

ランダム・マスク版AES回路に対して，シミュレーション上でDPA攻撃を行った例を**図16**に示します．理論的に完全でない面は残っているものの，攻撃の難易度を上げるには大きな効果があります．かぎの推定が合っている場合とまちがっている場合で平均電力差分がほぼ同じ形になるため，プロセス微細化に頼ったり，論理構成をBDDに変えたりするよりは，段違いに安全になると言えます．

● 実際に回路化するうえでの注意

この回路に限らず，ランダム・マスク法を利用するうえでは，回路中の各演算器の接続順序を崩さないようにしてください．対策の有効性に影響を与える場合があるからです．このため，各演算器をコンポーネント化したうえでフラッタリングせずに合成するなど，論理合成のやりかたにも気を配ってください．

最後に，システムLSIにセキュリティ処理を組み込むう

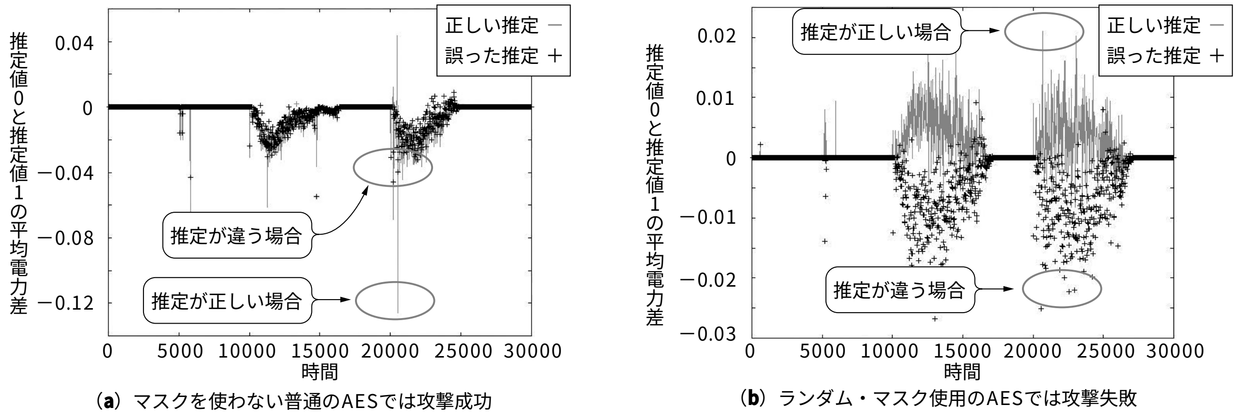


図16　ランダム・マスク化したAES回路のDPA攻撃例

(a) の普通のAES（合成体S-Box使用）では，シミュレーション上でDPA攻撃が可能だが，(b) のようにランダム・マスク化すると攻撃困難になる．実チップで微細プロセスの場合，マスクなしでも攻撃は容易ではないので，さらにランダム・マスク化すれば事実上攻撃できなくなると考えられる．

えで重要な点をまとめておきます．

- **“all or nothing”に走らない**――完ぺきなセキュリティを求め，それに多大なコストがかかるとわかると，今度はセキュリティを全部なくしてしまうというのはよくない
- **システム全体を見渡せる人がシステムLSIのセキュリティ機能の設計に加わる**――LSI設計の専門家とセキュリティの専門家のどちらか一方だけでは不十分．セキュリティにかかるコストが非現実的なものになったり，とんでもないセキュリティ・ホールができたりしやすい．

電力解析攻撃も同じ考えかたで扱うのがよいでしょう．

参考・引用*文献

(1) CRYPTREC暗号モジュール委員会・各年レポート，http://www.cryptrec.jp/report.html（この分野の研究動向がわかる）．
(2) スマートカードの安全性に関する調査，http://www.ipa.go.jp/security/fy11/report/contents/crypto/crypto/report/SmartCard/node39.html（若干古いが，整理された知識が得られる）．
(3) P. Kocher, J. Jaffe, and B. Jun ;“Differential Power Analysis”, Proc. CRYPTO ’99, LNCS Vol.1666, pp.388-397, 1999（DPAの原典）．
(4) 森岡澄夫ほか；合成体を用いたAES S-Box回路に対するDPA攻撃，情報処理学会・コンピュータセキュリティシンポジウム2004（CSS2004），pp.679-684（本稿の「AES暗号のRTLレベル対策法」で紹介した内容）．
(5) 市川哲也，鈴木大輔，佐伯稔；データマスクを利用したDPA対策に対する攻撃，信学技報，ISEC2004-58，pp.119-126，2004年．
(6) A. Satoh, S. Morioka, K. Takano and S. Munetoh ;“A Compact Rijndael Hardware Architecture with S-Box Optimization”, ASIACRYPT2001, LNCS Vol.2248, pp.239-254, Dec. 2001（合成体S-Boxの実装の詳細．同型写像の具体例も書いてある）．
(7) 和田知久，森屋和喜ほか；暗号回路設計のトライ＆エラー，Design Wave Magazine，2004年6月号，pp.91-113（AES暗号のS-Box回路や合成体）．
(8) 森岡澄夫；エラー訂正や暗号処理で使われる演算回路を究める，Design Wave Magazine，2003年7月号，pp.57-67（合成体の演算回路）．
(9) 森岡澄夫，佐藤証；共通鍵暗号AESの低消費電力論理回路構成法，情報処理学会論文誌，2003年5月号，pp.1321-1328，http://www.ie.u-ryukyu.ac.jp/~wada/design04/Morioka.pdf（AES暗号のS-Box回路）．
(10) 森岡澄夫；HDLによる高性能ディジタル回路設計，CQ出版社，2002年．

もりおか・すみお

<筆者プロフィール>
森岡澄夫．電話関連会社，コンピュータ関連会社，AV機器関連会社を経て，現在は大手電機メーカのLSI関連研究所勤務．エラー訂正・暗号・画像処理などいろいろな回路の研究と実開発を行ってきた中堅どころ．代表作はゲーム機のセキュリティ・システム回路など．
http://www02.so-net.ne.jp/~morioka/